Enhanced Cyber Risk Management Standards
Joint Response from Bank of Montreal (BMO) and Canadian Imperial Bank of Commerce (CIBC)

AGENCIES: The Board of Governors of the Federal Reserve System; the Office of the Comptroller of the Currency; and the Federal Deposit Insurance Corporation.

ACTION: Joint advance notice of proposed rulemaking.

SUMMARY: The Board of Governors of the Federal Reserve System (Board), the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) (collectively, the agencies) are inviting comment on an advance notice of proposed rulemaking (ANPR) regarding enhanced cyber risk management standards (enhanced standards) for large and interconnected entities under their supervision and those entities' service providers. The agencies are considering establishing enhanced standards to increase the operational resilience of these entities and reduce the impact on the financial system in case of a cyber event experienced by one of these entities. The ANPR addresses five categories of cyber standards: cyber risk governance; cyber risk management; internal dependency management; external dependency management; and incident response, cyber resilience, and situational awareness. The agencies are considering implementing the enhanced standards in a tiered manner, imposing more stringent standards on the systems of those entities that are critical to the functioning of the financial sector. Comments must be received by January 17, 2017.

Questions on the Scope of Application

	QUESTION	RESPONSE
1	How should the agencies consider broadening or narrowing the scope of entities to which the proposed standards would apply? What, if any, alternative size thresholds or measures of risk to the safety and soundness of the financial sector and the U.S. economy should the agencies consider in determining the scope of application of the standards? For example, should "covered entity" be defined according to the number of connections an entity (including its service providers) has to other entities in the financial sector, rather than asset size? If so, how should the agencies define "connections" for this purpose?	No recommendation to broaden the scope. In regard to connections, the size and systemic importance of an activity are better predictors of impact rather than the number of connections. It would be better to consider activities and their potential impact rather than focus on the channel. One or one-hundred channels (connections) could use the same secure control methodology\capability with the same outcome. More connections do not correlate to increased risk.
2	What are the costs and benefits of applying the standards to covered entities on an enterprise-wide basis? If the agencies were to consider exempting certain subsidiaries within a covered entity from the standards, what criteria should be used to assess any such exemptions? What safeguards should the agencies require from a subsidiary seeking to be exempted from the standards to ensure that an exempted subsidiary does not expose the covered entity to material cyber risk?	- The costs cannot be estimated using a linear methodology. The cost to implement will be directly related to the depth of activities between a Financial Institution and a covered entity. - Benefits of applying the Standards enterprise-wide - The benefit is parity for comparison - Exemption of subsidiaries - Each Financial Institution should compare it operations and capabilities to the Standards prior to making a case for special consideration. Exemptions should be considered with a focus on systemic impact. If an activity does not pose potential for excessive risk, it can be considered for exemption.
3	What, if any, special considerations should be made regarding application of the standards to savings and loan holding companies that engage significantly in insurance or commercial activities?	Exemptions for Savings and Loan organizations - Each Financial Institution should compare it operations and capabilities to the Standards prior to making a case for special consideration.

		Exemptions should be considered with a focus on systemic impact. If an activity does not pose potential for excessive risk, it can be considered for exemption.
4	What are the most effective ways to ensure that services provided by third-party service providers to covered entities are performed in such a manner as to minimize cyber risk? What are the advantages and disadvantages of applying the standards to services by requiring covered entities to maintain appropriate service agreements or otherwise receive services only from third-party service providers that meet the standards with regard to the services provided, rather than applying the requirements directly to third-party service providers?	Most effective ways to ensure third-parties minimize cyber risk - An effective third-party risk assessment activity is the most effective tool to assess third-party risk - Requiring covered entities to maintain service agreements that enforce the standards or limit providers to only those that meet the standards would provide practical challenges. Many vendors refuse to accept tighter contract terms – particularly those that are large, and those significant vendors where their market has less competition. Limiting third-party service providers to only those that are confirmed to meet the standards may increase the concentration of risk to fewer service providers.
5	What are the advantages and disadvantages of applying the standards directly to service providers to covered entities? What challenges would such an approach pose?	Applying standards directly to service providers Direct service provider oversight should be performed, in collaboration with each sectors' regulators, rather than directing their requirements at financial institutions. The Agencies seem to be placing the onus of responsibility on covered entities to drive third party compliance to these regulations, including those third parties in heavily regulated industries such as energy and telecommunications. We suggest that in line with Presidential Policy Directive 41 (PPD-41), that the Agencies work with other complimentary regulatory bodies for critical sectors to create a legislative and regulatory environment to support collective interests.
6	What factors are most important in determining an appropriate balance between protecting the safety and soundness of the financial sector through the possible application of the standards and the implementation burden and costs associated with implementing the standards?	Two lenses should be applied during consideration. The first is to allow an individual Financial Institution to mitigate risk to an acceptable level. The second is to aggregate potential impact across the system.

Questions on Sector-critical Systems

7	Do covered entities currently have access to sufficient information to determine whether any of their systems would be considered sector-	Clear guidelines must be established and understood by financial entities based on a global transactional volume of 5%, for example

	critical systems for the purpose of the standards? If not, what additional information would be necessary for an entity to identify whether it has one or more sector-critical systems for the purposes of the standards?	one entity may have significant impact globally in the case of failure but not necessarily in the United States. In addition, provisions should be granted in the case of a systemic IT failure for workarounds or manual processing methods that could be used as a risk mitigation.
8	What are the advantages and disadvantages of requiring covered entities to identify and report to the agencies their systems that support operations and meet the applicable thresholds to be considered sector-critical systems? Alternatively, what are the advantages and disadvantages of having the agencies develop a process to identify the systems of covered entities that support operations and meet the applicable thresholds to be considered sector-critical systems and to notify covered entities which of their systems would be subject to the sector-critical standards?	Agencies should collaborate and articulate the minimum requirements for a significant financial firm based on market share. Self-identification may result in an inconsistent application of the provisions.
9	What thresholds for transaction value in one or more critical financial markets should the agencies consider for identifying sector-critical systems? Similarly, what, if any, additional thresholds should the agencies consider for identifying sector-critical systems that could have a material impact on financial stability if disrupted? For example, how should the agencies identify systems that provide functionality to the financial sector and for which alternatives are limited, nonexistent, or would take excessive time to implement? How should such factors be weighted? Commenters are encouraged to provide quantitative as well as qualitative support and analysis for proposed alternative methodologies, thresholds and/or factors.	Thresholds for transaction value should not be based on a static monetary amount, rather a % of total market share/market materiality. In addition, telecommunications entities or payment processors should be also considered as part of the supply chain related to financial entities. Control evaluation to ensure robustness and business continuity health should be the focus for all critical financial services members and partners. Individual Financial Institutions don't have visibility into the volume or sensitivity of each channel. It would be better to see a proposal which could be assessed against the activities of each Financial Institution for review and response.
10	What are the advantages and disadvantages of determining that a covered entity which holds a substantial amount of U.S. deposits and/or balances due from other depository institutions in the United States plays a significant role in a critical financial market? At what level of activity should a covered entity's systems related to holding U.S. deposits and/or balances due from other depository institutions in the United States be determined to be critical to the sector?	A covered entity that holds significant US deposits/balances from other depository institutions should be governed by the same regulators as covered entities. This should include business continuity requirements.
11	What factors should the agencies consider in a measure of interconnectedness resulting in a system being determined as critical to the financial sector, and how should such factors be weighted? Commenters are asked to provide quantitative as well as qualitative support and analysis for proposed alternative methodologies, thresholds and/or factors.	Key factors for the evaluation of interconnectedness is the impact of operations and availability of access to funds. Should an entity cause operational harm to a covered entity, then the covered entity should enforce controls and evaluate health/compliance to control objectives.
12	In some cases, entities, such as smaller banking organizations, may provide services considered sector-critical services either directly to the financial sector or through covered entities. What criteria should the	The impact to the US market from smaller entities must be evaluated and a risk based assessment approach should be undertaken to determine true risk to the US market. Should material risk(s) exist due

	agencies use to evaluate whether a financial entity that would not otherwise be subject to the enhanced standards should be subject to the sector-critical standards? How should the agencies weigh the costs of imposing the sector-critical standards to such smaller banking organizations against the potential benefits to the financial system?	to a smaller entity providing sector-critical services, the costs should be appropriately estimated and understood to allow for healthy discussion and debate on potential risk mitigation options and how costs can be potentially addressed in a reasonable manner,

Category 1: Cyber risk governance

Questions on Cyber Risk Governance

13	How would a covered entity determine that it is managing cyber risk consistent with its stated risk appetite and tolerances? What other implementation challenges does managing cyber risk consistent with a covered entity's risk appetite and tolerances present?	An internationally recognized control framework exists (NIST CSF) and an internationally recognized operational capability framework exists (ISO 27001:2013), but no mature and recognized risk appetite/risk tolerance framework exists. Also, no quantitative framework for measuring risk is available. There are too many variables to create an acceptably accurate measurement of residual risk. All acceptable models are qualitative.
14	What are the incremental costs and benefits of establishing the contemplated standards for the roles, responsibilities, and adequate cybersecurity expertise (or access to adequate cybersecurity expertise) of the board of directors? To what extent do covered entities already have governance structures in place that are broadly consistent with the proposed cyber risk governance standards?	The costs are acceptable to ensure that the Board has access to cyber security expertise. Separately, governance structures are in place with the caveat mentioned in question 13. No mature risk appetite framework is a challenge. Each organization creates its own version of aggregate risk measurement and tolerance. Also, no quantitative framework for measuring risk is available. There are too many variables to create an acceptably accurate measurement of residual risk. All acceptable models are qualitative.

Category 2: Cyber risk management

Questions on Cyber Risk Management

15	The agencies seek comment on the appropriateness of requiring covered entities to regularly report data on identified cyber risks and vulnerabilities directly to the CEO and board of directors and, if warranted, the frequency with which such reports should be made to various levels of management. What policies do covered entities currently follow in reporting material cyber risks and vulnerabilities to the CEO and board of directors?	The standards for covered entities should mirror Financial Institutions. And, not all risks are worthy to be reported to the CEO and Board of Directors. Policies will vary by organization and the sensitivity of the provided activity.
16	The agencies seek comment on requiring covered entities to organize	No Further Suggestions

	themselves in a manner that is consistent with the contemplated enhanced standards for cyber risk management. Besides the approach outlined in the ANPR, what other approaches could ensure that entities are effectively monitoring, measuring, managing, and reporting on cyber risk?	

Category 3: Internal dependency management; and
Category 4: External dependency management

Questions on Internal and External Dependency Management

17	The agencies request comment on the comprehensiveness and effectiveness of the proposed standards for internal and external dependency management in achieving the agencies' objective of increasing the resilience of covered entities, third-party service providers to covered entities, and the financial sector.	Internal Dependency Management The proposal is overly comprehensive in requiring all internal assets and business functions, including mappings to other assets and business functions, information flows and interconnections. Refinement around scope is needed to allow for a risk-based approach. Recommend that this standard be revised to a more reasonable and realistic standard applied to assets deemed to be most material and posing a high probability of cybersecurity risk; assessment of assets and their associated risks should be conducted and improvements made on a periodic basis, or when material risks have changed. External Dependency Management As written, this suggests that the requirements in this standard would apply to all third parties, including vendors, with which a financial institution works, regardless of the level of connectivity (or lack thereof) to the institution's systems or information; by default, this would also apply to energy and telecommunications providers, industries that themselves are already heavily regulated and who share the same interest in cybersecurity.
18	What challenges and burdens would covered entities encounter in maintaining an internal and external dependency management strategy consistent with that described by the agencies?	The outlined approach is exceedingly broad, and would require significant administrative overhead.
19	How do the proposed internal and external dependency management standards compare with processes already in place at banking organizations?	In keeping with existing federal regulations and industry best-practice guidelines, large financial institutions have mature risk-based processes and governance frameworks to manage all levels of operational and financial risks. Overly prescriptive regulations for

		internal and external dependency management applicable to all assets, third parties and interconnections, regardless of their level of risk or relationship to sector-critical systems, would add more complexity and administrative overhead that far outweighs the benefits suggested by the Agencies.
20	What other approaches could the agencies use to evaluate a covered entity's internal and external dependency management strategies? Please be specific as to each approach.	Entities have existing evaluative processes that are structured under the aforementioned three lines of defense risk-management model. The existing FFIEC Cybersecurity Assessment Tool (CAT) has been used by all large financial institutions within the last 12-18 months to gauge the level of maturity of in-place cybersecurity programs, and most entities have initiatives underway to close any gaps identified with this useful tool.
21	How would the proposed standards for internal and external dependency management impact a covered entity's use of a third-party service provider?	Under current requirements, many vendors refuse to accept tighter contract terms – particularly those that are large, and those significant vendors where their market has less competition. Under the ANPR, financial institutions are required to negotiate numerous controls in contracts with third parties, including rights for on-site audits and real-time monitoring. This makes innovation challenging, as many service providers offer unique services in fields with limited competition, such that financial institutions lack the negotiating power to demand strict contractual terms. Additionally, the requirement to "continually apply and evaluate appropriate controls" suggests a non-stop process of evaluation; we suggest that periodic assessments are more reasonable and appropriate until automated continuous monitoring becomes practical. Another concern is real-time monitoring of the universe of external dependencies and trusted connections. In the large and complex environments at most large financial institutions, to monitor all such connections is a significant ask, requiring significant resources in terms of personnel and funding. We recommend that any monitoring requirements be relegated to only the systems or interconnections to defined sector-critical systems, and utilities such as energy and telecommunications be excluded from the external dependency definition.
22	What additional issues should the agencies consider related to internal and external dependency management and the covered entities' use of third-party service providers? How should those issues be evaluated by the agencies? Please be specific.	Rather than adding continuously stringent vendor oversight requirements, the agencies can strengthen the financial sector's resiliency by strengthening the resiliency of the underlying service providers and infrastructure backbone.

		Any further service provider requirements should be considered for implementation through direct service provider oversight, in collaboration with each sectors' regulators, rather than directing requirement at financial institutions. The Agencies seem to be placing the onus of responsibility on covered entities to drive third party compliance to these regulations, including those third parties in heavily regulated industries such as energy and telecommunications. We suggest that in line with Presidential Policy Directive 41 (PPD-41), that the Agencies work with other complimentary regulatory bodies for critical sectors to create a legislative and regulatory environment which mandates telecommunications providers perform reasonable steps to proactively block known malicious internet traffic and disconnect "bad actors" without fear of liability.

Category 5: Incident response, cyber resilience, and situational awareness

Questions on Incident Response, Cyber Resilience, and Situational Awareness

23	How well do the proposed standards for incident response, cyber resilience, and situational awareness address the safety and soundness of individual financial institutions and potential systemic cyber risk to the financial sector, including with respect to the testing strategies and approaches? How could they could be improved? Standards within the incident response, cyber resilience, and situational awareness category would be designed to ensure that covered entities plan for, respond to, contain, and rapidly recover from disruptions caused by cyber incidents, thereby strengthening their cyber resilience as well as that of the financial sector. Covered entities would be required to be capable of operating critical business functions in the face of cyber-attacks and continuously enhance their cyber resilience. In addition, covered entities would be required to establish processes designed to maintain effective situational awareness capabilities to reliably predict, analyze, and respond to changes in the operating environment.	Components of Cyber Resilience should be clearly defined. For example: - Technology Resilience (covering: internal operations, outsourced services where bank is providing service, outsourced services where bank is receiving services) - Business Resilience - Traditional Kinetic (Physical and Environmental) Resilience - Communication and Education Resilience --- The following content is not clear: "..thereby strengthening their cyber resilience as well as that of the financial sector." Does this mean that all information on covered entity's disruption must be shared with broader FI community? Are there any categories based on financial impact associated with disruption that can be used to differentiate

		what information should be shared? Potential financial impact if new requirement mandate that technology supporting critical business functions must have a "hot standby switch" capability to resume seamlessly operations while cyber attack is ongoing.
	The agencies are considering a requirement that covered entities establish and maintain effective incident response and cyber resilience governance, strategies, and capacities that enable the organizations to anticipate, withstand, contain, and rapidly recover from a disruption caused by a significant cyber event. The agencies are considering a requirement that covered entities establish and implement plans to identify and mitigate the cyber risks they pose through interconnectedness to sector partners and external stakeholders to prevent cyber contagion.	Need clarity on the definition of "significant cyber event" (for example, for FI-A having a MM$10 cyber event could be Low, and for their business partner or FI-B the same event could be Catastrophic). Not clear who "sector partners and external stakeholders" are. "Capacity" to withstand and recover from a severe cyber event should be a risk-based decision. "Rapidly recovery" is an aspiration that is not well-defined. New term "safe recovery" may offer covered entity ability to ensure disrupted environments are safely recovered. Potential financial impact for "interconnectedness to sector partners and external stakeholders to prevent cyber contagion".
	In addition, the agencies are considering a requirement that covered entities establish and maintain enterprise-wide cyber resilience and incident response programs, based on their enterprise-wide cyber risk management strategies and supported by appropriate policies, procedures, governance, staffing, and independent review. These cyber resilience and incident response programs would be required to include effective escalation protocols linked to organizational decision levels, cyber contagion containment procedures, communication strategies, and processes to incorporate lessons learned back into the program.	Potential financial impact for global-scalability, staffing, and independent review. Not clear on who can execute independent review and frequency.
	Cyber resilience strategies and exercises would be required to consider wide-scale recovery scenarios and be designed to achieve institutional resilience, support the achievement of financial sector-wide resilience, and minimize risks to or from interconnected parties. The IT Handbook calls for examiners to determine whether covered entities have established plans to address recovery and resilience strategies for cyber-attacks that may disrupt access, corrupt data, or destroy data or systems. In addition to establishing recovery time objectives (RTOs), recovery and resilience strategies should address the potential for malware or corrupted data to replicate or propagate through connected systems or high availability solutions. For cyber-attacks that may	Potential financial impact for various exercises and global-scalability. Not clear on definitions for "institutional resilience", "financial sector-wide resilience", and "interconnected parties". Everything that goes beyond covered entity adds complexity that needs to be managed by a central entity. The intent here does not offer guidance on central entity for financial sector-wide resilience.

	potentially corrupt or destroy critical data, recovery strategies should be designed to achieve recovery point objectives based on the criticality of the data necessary to keep the institution operational.	
	In this category, the agencies also are considering a requirement that covered entities establish and implement strategies to meet the entity's obligations for performing core business functions in the event of a disruption, including the potential for multiple concurrent or widespread interruptions and cyber-attacks on multiple elements of interconnected critical infrastructure, such as energy and telecommunications.	The intent goes beyond cyber-related topic " including the potential for multiple concurrent or widespread interruptions and cyber-attacks on multiple elements of interconnected critical infrastructure"
	The preservation of critical records in the event of a large-scale or significant cyber event is essential to maintaining confidence in the banking system and to facilitating resolution or recovery processes after a catastrophic event. The agencies are therefore considering requiring covered entities to establish protocols for secure, immutable, off-line storage of critical records, including financial records of the institution, loan data, asset management account information, and daily deposit account records, including balances and ownership details, formatted using certain defined data standards to allow for restoration of these records by another financial institution, service provider, or the FDIC in the event of resolution.	Potential financial impact and security risk for this backup-service. Reasonable intent, lacks details with respect to who is defining data standards, unknown impact to operations of a covered entity operating in other Countries. Similar to FS-ISAC Sheltered Harbor initiative. The ability to preserve data integrity is important. However, it could be excessively expensive to expect migration across multiple systems when a data standard is created and enforced by a Regulatory Agency assuming that a single standard can be created.
	Transition plans are essential in the event a service is terminated or an entity cannot meet its obligations. Thus, the agencies are considering a requirement that covered entities establish plans and mechanisms to transfer business, where feasible, to another entity or service provider with minimal disruption and within prescribed time frames if the original covered entity or service provider is unable to perform. As a result, if performance is not feasible and contractual termination/remediation provisions have been exercised, client data would be returned to the original covered entity or service provider in a method that is transferable to an alternate entity or service provider with minimal disruption to the operations of the covered entity.	Reasonable intent, lacks detail to fully determine impact. Potential financial impact and security risk for this external service. The concept of moving data and operations for execution to another entity in a crisis could cause further risk during a crisis and speed up the downfall of a covered entity. This could create risk and instability. Providers may choose to end contracts and services if they are required to collaborate with competitors. Also, it will generate an excessive expense to existing contracts and services.
	Testing the cyber resilience of operations and services helps to identify potential threats to the ongoing performance of the operation or service. A prolonged disruption of a significant operation could generate systemic	

	risk. The agencies are considering a requirement that covered entities conduct specific testing that addresses disruptive, destructive, corruptive, or any other cyber event that could affect their ability to service clients; and significant downtime that would threaten the business resilience of clients. In addition, the agencies are considering a requirement that the testing address external interdependencies, such as connectivity to markets, payment systems, clearing entities, messaging services, and other critical service providers or partners; that the testing of cyber resilience be undertaken jointly where critical dependencies exist; and that the testing validate the effectiveness of internal and external communication protocols with stakeholders. A key element of situational awareness is the timely identification, analysis, and tracking of data about the state of, and potential cyber risks to, the organization. The agencies are considering a requirement that covered entities maintain an ongoing situational awareness of their operational status and cybersecurity posture to pre-empt cyber events and respond rapidly to them. Covered entities also would be required to establish and maintain threat profiles for identified threats to the firm; establish and maintain threat modeling capabilities; gather actionable cyber threat intelligence and perform security analytics on an ongoing basis; and establish and maintain capabilities for ongoing vulnerability management.	Reasonable intent, lacks needed detail to determine impact. Potential financial impact on rewriting business contracts with suppliers and partners. Reasonable intent, lacks detail to fully determine impact. Pre-empt cyber events could be a tie into Threat Hunting and Threat Intelligence. Threat profiles would need further clarification, larger covered entities have mature Operational Risk practices that include a component of Scenario planning.
24	What is the extent to which it would be operationally and/or commercially feasible to comply with requirements to use certain defined data standards in order to increase the substitutability of third-party relationships to reduce recovery times for systems impacted by a significant cyber event?	Further details required. Not feasible operationally and/or commercially due to global operations of the covered entities, and potentially the covered entity's suppliers, within scope of the ANPR. ANPR proposed Data Standards would need to be ratified and adopted globally to ensure consistency in all jurisdictions.
25	How do covered entities currently evaluate their incident response and cyber resilience capabilities? What factors should the agencies consider essential in considering a covered entity's incident response and cyber response capabilities?	Covered entities have an opportunity to participate in industry-led Cyber Resilience testing, such as the SIFMA-led exercises testing Cyber response. In addition, Operational Risk practices include a component of Scenario planning and table top exercises. These following factors should be considered: - Response scenario-driven plans - Containment plans - Recovering plans - Exercising the above plans - Enhancing capabilities with lessons learned from the planning and exercising
26	How do covered entities currently evaluate their situational awareness	By establishing threat intelligence (includes threat hunting) and

	capabilities? What factors should the agencies consider essential in considering a covered entity's situational awareness capabilities?	vulnerability management functions. These functions need to reach out to threat and vulnerability source for harvesting information on the latest threats and vulnerability that can be processed and actioned for internal consumption. These following factors should be considered: - Cyber Threat Intelligence function - Vulnerability Management function - External sources for Intelligence threat community (includes Industry partners, Law Enforcement) - External sources for Vulnerability research community - Common severity, appetite and risk-based enterprise levels - Common vulnerability scoring enterprise methods - Common intel and vulnerability reporting format/methods/frequency - Centralized repository for management of findings and their risk treatments (and associated remediation plans if applicable) - Measurements, performance, CMM monitoring and reporting
27	What other factors should be included within the incident response, cyber resilience, and situational awareness category?	The following factor should be considered: - Preserving the Chain of Evidence for incidents
28	What additional requirements should the agencies consider to improve the resilience or situational awareness of a covered entity or the ability of a covered entity to respond to a cyber-attack?	See comments provided above in response to question 23.

Questions on Standards for Sector-Critical Systems of Covered Entities

29	The agencies request comment on the appropriateness and feasibility of establishing a two-hour RTO for all sector-critical systems. What would be the incremental costs to covered entities of moving toward a two-hour RTO objective for these systems?	• Costs and effort would be likely be very high, and very expensive to implement based on the information provided. Actual costs would vary depending on the overall decision of the agencies scope for RTOs • Time to implement a 2 hour RTO would involve multi-year programs which may require development of independent instances of platforms running in parallel in geographically and logically separate zones • Requiring a 2 hour RTO on critical systems would likely require

		companies to defer investment in other technology areas including currency initiatives, new product development, etc.
30	What impact would a two-hour RTO have on covered entities' use of third-party service providers? What challenges or burdens would be presented by the requirement of a two-hour RTO for covered entities who rely on third-party service providers for their critical systems? How should the agencies weigh such costs against other costs associated with implementing the enhanced standards outlined in this ANPR?	• The primary challenge would be to influence service to implement changes to their systems that would allow for a 2 hour RTO. • Financial institutions would not have the authority to be able to insist on this requirement to third party providers over the course of current contracts – 2 hr RTO could be negotiated in new contracts and vendors would need lead time to build this functionality into current solutions. • Another significant challenge may be aligning the third party provider and our systems to work "end to end" in a 2 hour RTO scenario. Providers may or may not allow that kind of integration/knowledge with their systems • Analysis, design and implementation of these changes would likely take a significant amount of time and cost to implement. • Providers vary in size, funding and ability. Some vendors may not be able to afford to comply with the RTO.
31	How should the agencies implement the two-hour RTO objective? For example, would an extended implementation timeline help to mitigate costs, and if so, what timeline would be reasonable?	• Agencies should work with individual institutions to understand costs, and timelines appropriate for each. Not all entities would be willing/able to implement all changes as they vary in size and abilities. A one size fits all solution is likely not tenable • Extended timelines would certainly help to mitigate costs, but understanding what those timelines would be would need to be based on a deep analysis of the scope of the gap, efforts required to implement, and ability to implement • Multi-year timelines (e.g. 7 – 10 years) would be required to effect industry and third party compliance.
32	Should different RTOs be set for different types of operations and, if so, how? Should RTOs be expected to become more stringent over time as technology advances?	• RTOs should be set and implemented following a risk based approach • Higher risk systems that could affect the financial sector should face different RTO's from lower risk systems that have minor or little impact • The goal should not necessarily be a specific pre-defined RTO number, but rather the RTO number that makes sense to minimize impact on the financial system. • The goal should also not be to make RTOs more stringent over time as technology advances, but rather have the most appropriate RTO based on a risk based approach to minimize impact on the financial system.
33	The Board requests comment on the benefits of requiring Board-supervised covered entities, at the holding company level, to measure the residual cyber risk of their sector-critical systems on a quantitative	• This would require significant investment and effort to define appropriate tools and KRI's to measure residual risk on-going and in real-time. At this time, no effective quantitative model exists to

	basis. How would this approach to measuring cyber risk compare with efforts already underway at holding companies to manage and measure their cyber risk? For example, what processes do holding companies already have in place to measure their residual cyber risk? What challenges and costs would holding companies face in measuring their residual cyber risk quantitatively? What are the benefits of requiring holding companies to reduce the residual risk of their sector-critical systems to a minimal level, taking into account the risks associated with internal and external dependencies connected to or supporting their sector-critical systems?	measure residual risk. • Cyber risk today is measured at an enterprise level with enterprise KRIs at most organizations. Methods to measure residual cyber risk of sector-critical systems differ between organizations and are inconsistent, generally limited in maturity, or may not performed at all. • There is benefit in reducing residual risk of sector-critical systems, however, the closer we can get to zero risk, the exponentially more expensive the remediation will cost. Reduction of residual risk could act as a deterrence to external threat actors.

Questions on Approach to Quantifying Cyber Risk Section

34	What current tools and practices, if any, do covered entities use to assess the cyber risks that their activities, systems and operations pose to other entities within the financial sector, and to assess the cyber risks that other entities' activities, systems and operations pose to them? How is such risk currently identified, measured, and monitored?	• Currently, examples of common tools and practices include business impact analysis, scenario analysis, risk assessments, supplier risk assessments, and technical security testing (e.g. vulnerability scans, penetration tests). These tools and practices are mostly qualitative tools.
35	What other models, frameworks, or reference materials should the agencies review in considering how best to measure and monitor cyber risk?	• Approaches that use NIST Cyber Security Framework as a basis to organize detailed controls and associated measurement and monitoring guidance. • Other risk management frameworks include NIST SP800-37 or ISO 27001
36	What methodologies should the agencies consider for the purpose of measuring inherent and residual cyber risk quantitatively and qualitatively? What risk factors should agencies consider incorporating into the measurement of inherent risk? How should the risk factors be consistently measured and weighted?	There are several methodologies that should be considered including: • Harmonized TRA Methodology (Communications Security Establishment – Canada) • NIST SP-800-37 • ISO 27001 • ISO 31000 • ISF IRAM2 The above methodologies and frameworks provide a variety of impact and likelihood factors that should be considered. The adoption of a consistent methodology that can be used industry-wide would require that it be comprehensive, adaptable to evolving threats, and relevant and valuable to organizations of different sizes. The additional challenge of differing risk tolerances across entities will need to be considered such that risks can be translated between entities of different sizes, especially in cases where there are external dependencies involved.

Questions on Considerations for Implementation of the Enhanced Standards

37	What are the potential benefits or drawbacks associated with each of the options for implementing the standards discussed above?	Covered entities should be allowed to adapt their environments to the needs of their business, improving their risk management and mitigation processes according to an evolving threat landscape.
38	What are the trade-offs, in terms of the potential costs and other burdens, among the three options discussed above? The agencies invite commenters to submit data about the trade-offs among the three options discussed above.	See prior Overall Commentary
39	Which approach has the potential to most effectively implement the agencies' expectations for enhanced cyber risk management?	Any potential standards must focus upon objectives and end-goals, rather than prescriptive mandates for achieving desired outcomes. Entities must be afforded the flexibility to achieve set objectives in a manner that best reflects and benefits their respective operating and organizational environments. Additionally, we again recommend that a risk-based approach be adopted, rather than more prescriptive requirements which may not need to be applied to low-criticality assets and processes.